IN THE ABSTRACT

Please add the following Abstract:

ABSTRACT

The invention relates to a cryptographic method involving an integer division of type q = a div b and r = a mod b, wherein a is a number of m bits, b is a number of n bits, with n being less than or equal to m, and b_{n-1} being non-null and the most significant bit of b. In addition, each iteration of a loop subscripted by i, which varies between 1 and m-n+1, involves a partial division of a word A of n bits of number a by number b in order to obtain one bit of quotient q. According to the invention, the same operations are performed with each iteration, regardless of the value of the quotient bit obtained. In different embodiments of the invention, one of the following is also performed with each iteration: the addition and subtraction of number b to/from word A; the addition of number b or a complementary number /b of b to word A; or a complement operation at 2^n of an updated datum (b or /b) or a dummy datum (c or /c) followed by the addition of the datum updated with word A.